Scale the Solution to the Problem

Campuses need to move proactively to meet growing information security demands

By **Cedric Bennett**

The only way of discovering the limits of the possible is to venture a little way past them into the impossible.[1]

Arthur C. Clarke

The Internet is a remarkable tool and change agent that has been successfully leveraged by colleges and universities to support, enhance, and extend the teaching/learning process; the creation of new knowledge through research; and the increasingly complex business of managing and administrating our institutions. Moreover, it has become an indispensable communications mechanism through which we reach students, faculty, staff, donors, alumni, applicants, granting agencies, vendors, the public, and others.

At the same time that the Internet has become a mission-critical resource, it has also introduced new and growing responsibilities. Although it supports and even creates new ways to enhance the education process, this virtually unregulated communications medium has also become a costly management burden. It is becoming a more difficult environment to use safely—the ability to reach out to the rest of the world also invites the rest of the world to reach back, sometimes in very unsettling ways. And, as if the threat of unprovoked cyber attack were not enough to manage, federal and state legislation designed primarily to protect individual privacy has been demanding additional resource allocation with increasing frequency.

Increasing Cyber Threats

Ever since Robert Morris wrote the first computer worm in 1988,[2] information-security experts have been both observing and defending against a growing number of Internet attacks. What is becoming increasingly clear is that the level, sophistication, speed, and time-to-exploit of autonomous Internet-based attacks are escalating. A few examples of the increase of serious and debilitating network exploits occurring in 2003 alone illustrate how grave the situation has become:

- *Speed of delivery*—The MS SQL Slammer worm traversed the entire Internet and did nearly all of its damage in less than 15 minutes, whereas previous rapidly spreading exploits took multiple hours or days to infect targets worldwide.

- *Vulnerability of private information*—The BugBear virus/worm showed just how vulnerable our institutions' widely distributed data is by sending very private or confidential letters and files, located on campus-wide desktop computers, to unauthorized recipients all over the world.
- *Sophistication and speed of delivery*—SoBig showed just how easily and rapidly an e-mail-delivered virus/worm could evade antivirus software and invade and replicate itself onto nearby machines.
- *Sophistication of payload and time-to-exploit*—Blaster, and nearly a dozen other MS RPC exploits, began appearing only two weeks after the vulnerability had been announced and the patch made available by Microsoft,[3] and it delivered a very sophisticated, multi-pronged, and expensive attack.[4]

Increasing Unfunded Regulatory Mandates

Most universities and colleges are aware of the FERPA regulations regarding the protection of certain elements of student information; these requirements have been a well-known part of the higher education regulatory environment for multiple decades. However, within the past several years federal legislation (and in some cases state legislation) has added an almost debilitating array of additional privacy and security requirements. Some of the major ones follow:

- FERPA—Family Educational Rights and Privacy Act of 1974; also known as the Buckley Amendment
- HIPAA—Health Insurance Portability and Accountability Act of 1996
- DMCA—Digital Millennium Copyright Act of 1998
- GLBA—Gramm-Leach-Bliley Act of 1999
- USA PATRIOT Act—Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
- TEACH Act—Technology, Education, and Copyright Harmonization Act of 2002

Others, less recent but still very significant, include the Electronic Communications Privacy Act of 1986 and the Computer Fraud and Abuse Act of 1986.

Each of these federal laws includes both management and information technology requirements. In some cases, there are even new institutional roles required (such as privacy officer, security officer, security plan coordinator, and notification of claimed infringement agent). Congress does not seem to feel that they have finished this work; more legislation requiring even more attention to privacy and information security is being proposed and considered today.[5]

Shifting Toward a Proactive Stance

As these threats and compliance requirements have increased, more and more of our institutions have focused on improving their information-security posture. Probably the single greatest movement forward has come about as a result of shifting to a proactive stance. Instead of just reacting to problems and incidents as they occur, colleges and universities are starting to think in terms of anticipating issues and working to prevent them. Another major shift forward has come from a growing realization that information security and regulatory compliance is not just a technology issue but is broadly institutional and very people-focused.[6]

Some of our institutions have designated specific individuals as security officers and created small teams to focus on information security. Others have assigned the information-security role as a collateral duty of one or more staff members. No matter how the function is staffed, those individuals charged with attending to information security and compliance are adopting a variety of approaches to leverage their resources and technical expertise, all aimed at improving the information-security posture of their institution. They know they don't have sufficient resources to meet all challenges alone; many of the solutions these information-security leaders choose include creating and leveraging strategic alliances with others across their institutions. What follows are examples of some key approaches being applied.

Build Alliances

Wise information-security officers understand that other staff offices within the institution are also responsible for aspects of compliance, protection of data, development of policy, interpretation of law, and like activities. Some of these functions may be staffed within the college or university, and some may be outsourced. In addition, there are often committees made up of faculty, students, and staff with advisory or oversight responsibilities in at least some of these same areas. The organizational names may vary, but they usually cover such functions as internal audit, general counsel, compliance, risk management, and public safety.

In any case, no matter what they are called or how they are staffed, these are key offices engaged in information-security–related activities. At the very least, they are experts in specific disciplines, which can be useful in providing crucial answers or interpretations to questions of law, business, risk, research, security, and so on. From a more strategic perspective, they can also become partners in helping to present and support information-security solutions to other campus leaders.

Identify Key Data Owners

Major administrative offices in most institutions are responsible for much of the institution's data, which can include (but is not limited to) financial, personnel, student, fund-raising, investment, and compliance data. Just as critical, but often far less centrally managed, is research data, course data, and other intellectual capital of the institution or individuals.

The individuals and offices charged with the responsibility for institutional data care a great deal about its protection. Because they are not focused primarily on information security, however, they often are not aware of the variety of cyber threats that may exist. Security officers who have invested the time to identify, meet, and educate these leaders usually find them willing allies in presenting and implementing information-security measures.

Create Partnerships

Others outside of the central security organization have both responsibility

for and expertise with information security—at least with regard to their specific responsibilities. These individuals may work in other parts of the central computing organization, or they might be located in widely distributed parts of the institution in academic or administrative organizations or research laboratories. Establishing liaison with these individuals goes a long way toward extending the knowledge and influence of any central security organization. Developing these distributed experts into a peer group that shares information, deals with serious emergencies, and reviews ideas for improving information security works to overcome the boundaries that can otherwise prevent meaningful dialogue and cooperation.

Similarly, connections can be established with other information-security practitioners working in other institutions, so that difficult questions can be considered from a variety of perspectives. Joining online discussion lists like the EDUCAUSE Security Discussion Group (http://www.educause.edu/security) or attending annual conferences like the EDUCAUSE/Internet2 Security Professionals Workshop (http://www.educause.edu/conference/security/) are excellent ways to meet and leverage the expertise of others working on similar problems at other institutions.

Set Institutional Policies

Every information-security officer knows that policies alone don't stop hackers or protect institutional data. But effective information-security officers also know that policies create the context and the foundation for developing the practices that can accomplish those goals.

Establishing institutional policies can be a time-consuming job. The advantage, however, is that not only do these important polices get written and accepted, the very process can help in raising awareness and educating others.

Raise Information Security Consciousness on Campus

Raising awareness of information-security issues across the campus is a must. The goal is not to make every computer user an expert in information security. Rather, the effort aims to make every computer user aware that information security is an important issue and one in which each of them must play a role. The objective is to help develop simple but effective habits that will raise institutional information security—similar to an educational campaign to make sure everyone uses a deadbolt to lock exterior doors on their homes.

Increase Technical Expertise

Security officers know that they cannot raise the level of campus information security single-handedly. Just as it is important to raise overall awareness of information security across the institution so that each individual can contribute to the solution, it is critical to raise the level of detailed information-security expertise among technical staff. Only through such education and training will more effective practices be broadly exercised in the deployment of both central and distributed information resources. The information-security staff will normally be the experts to those experts—it is the system administrators, programmers, database administrators, and others who will successfully follow effective practices that ensure a successful information-security program.

Only Deploy Technologies with the Greatest Leverage

Technology is important to successful information security, but it does not play as major a role as the issues mentioned above. Vendors often promise wonderful results from the simple deployment of their hardware or software solutions. Security officers understand that they should only deploy technology with proven value that can be managed with a minimum of resources.

Reexamine Underlying Assumptions

In most of our institutions, approaches to information security have not kept pace with the problems. As the examples provided at the beginning of this article illustrate, the growth in the scale, scope, tenacity, and costs of the issues we face are all rapidly increasing. It is unlikely that minimalist, reaction-based, or single-point-oriented solutions will succeed in addressing these complex problems. Moreover, such solutions will almost certainly not prove effective against problems we have yet to see.

The more broadly based approaches outlined in the section above have greatly helped the institutions implementing them. They are both proactive and strategic in approach, which tends to help in the development of solutions that are more general and effective over a larger set of problems. Still, these information-security solutions are frequently implemented in a general atmosphere that is not particularly tolerant of what are often perceived to be unnecessary and bureaucratic restrictions.

In higher education there is often a natural tension between the fundamental mission and culture of the institution, which encourages and thrives on open sharing and communication, versus the fiduciary and legal requirements of those same institutions to keep certain kinds of information resources secure and confidential. This tension has been balanced and handled with varying degrees of success at different institutions. On some of our campuses there is an understanding that it is important at least to acknowledge the tension and recognize that there will be times when both of those requirements may not be fully served.

It is important to begin discussion on our campuses aimed at developing a strategy that meets the institutional need for information security and also supports the requirements of the institution to successfully pursue its fundamental mission of teaching, learning, research, and public service. Such a discussion will not be easy to start or maintain; it is a leadership task that will take collaborative effort across the entire institution. It will include addressing knotty issues:

- Reconsidering decisions made in the past, when threats and requirements were not as severe as they have become today
- Confronting conventional wisdom about the specific requirements for

openness and the real versus imagined constraints imposed by information-security technologies
- Developing institutional information-security policies and an information-security architecture
- Recognizing that sensitive information exists in digital form all across and even beyond the campus, from highly secure servers to traveling laptop computers
- Discovering where real needs exist for reduced security (for example, specific research projects) and providing such facilities while protecting all other resources
- Acting from the understanding that information security is more a people issue than a technical one and that education and communication are a major part of any solution
- Seeking ways to support information-security requirements that are engineered to minimize both dependence upon individual conformity and overly oppressive controls

Each institution will need to find the solutions that best suit its own values and goals as well as its legal requirements, view of acceptable risk, and budget constraints. These discussions can be guided by a set of principles recently articulated by a National Science Foundation–sponsored workshop organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force:[7]

- Civility and community
- Academic and intellectual freedom
- Privacy and confidentiality
- Equity, diversity, and access
- Fairness and process
- Ethics, integrity, and responsibility

A major advantage of this effort to develop an institutional information security strategy is the knowledge that the outcome will be an informed institutional decision that is owned and understood throughout the campus.

Probably the best news is that general attitudes about the need for information security are shifting more toward the positive. The members of our community and our institutional leaders are becoming more acutely aware of just a few of the serious consequences of inadequate protection or insufficient regulatory compliance. Many are now ready to support recommendations that will lead to a more secure information environment on our campuses.

Our campuses now need information-security leaders with the courage to start the difficult dialogue, the understanding to keep the conversation focused on institutional requirements, and the insight to manage the discussion within that institutional context. *e*

Endnotes

1. Clarke's "second law," from A. C. Clarke, *Profiles of the Future: An Inquiry into the Limits of the Possible* (London: Gollancz, 1999, updated edition).
2. On November 2, 1988, Robert Morris, Jr., a graduate student in computer science at Cornell University, wrote an experimental, self-replicating, self-propagating program called a worm and injected it into the Internet.
3. By comparison, the MS SQL Slammer worm of early 2003 exploited a vulnerability for which a patch had been available for six months.
4. Many relatively well-prepared universities saw upwards of 30 percent of their Windows machines infected by the MS RPC exploits. The cost of repair plus the cost of lost productivity for these institutions is in the multi-million-dollar range.
5. I do not argue that such legislation is inappropriate or unnecessary, only that it is increasing the information-security management and cost burden of our institutions.
6. D. Ward, "Letter to Presidents Regarding Cybersecurity," ACEnet, Eye on Washington, Feb. 28, 2003; on the Web at <http://www.acenet.edu/washington/letters/2003/03march/cyber.cfm>.
7. EDUCAUSE/Internet2 Computer and Network Security Task Force, "Principles to Guide Efforts to Improve Computer and Network Security for Higher Education," August 2002; on the Web at <http://www.educause.edu/ir/library/pdf/SEC0310.pdf>.

Cedric Bennett (Ced.Bennett@stanford.edu) is Emeritus Director, Information Security Services, at Stanford University in Stanford, California, and still spends considerable time helping Stanford and other institutions address their information security requirements.